

FILED

MAY 13 2020

PETER A. MOORE, JR., CLERK
US DISTRICT COURT, EDNC
BY PC DEP CLK

UNITED STATES DISTRICT COURT

for the
Eastern District of North Carolina

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)iPhone located at
721 Medical Center Drive, Suite 300, Wilmington, North
Carolina 28401

Case No.

7:20-mj-1102-RJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location).
See Attachment Alocated in the Eastern District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

iPhone (IMEI # 356598080041281) located at 721 Medical Center Drive, Suite 300, Wilmington, North Carolina 28401

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2252AOffense Description
Distribution, Receipt, and/or Possession Child PornographyThe application is based on these facts:
See attached affidavit which is attached hereto and incorporated herein by reference

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

On this day, Addy Penniman
appeared before me via reliable electronic means, was
placed under oath, and attested to the contents of this
Application for a Search Warrant.Date: May 13, 2020City and state: Wilmington, North Carolina

Applicant's signature

Addy Penniman, Special Agent, HSI

Printed name and title



Judge's signature

Robert B. Jones, Jr., United States Magistrate Judge

Printed name and title

BMS

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Addy Penniman, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating Andrew HUFF for offenses related to child sexual exploitation. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search a silver/white iPhone (the "SUBJECT DEVICE"), that is located at HSI Wilmington, 721 Medical Center Drive, Suite 300, Wilmington, North Carolina 28401 and specifically described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment B.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located on the SUBJECT DEVICE.

BMS

AFFIANT BACKGROUND

3. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to Wilmington, North Carolina and have been so employed since August 2009. I am responsible for investigations involving the production, importation, advertising, receipt, and distribution of child pornography which occur in the Eastern District of North Carolina. I have participated in over 200 child pornography investigations. I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received training in the area of child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes. I have also received specialized training from Internet Crimes Against Children Task Force seminars and at the Dallas, Texas Advocacy Center's Crimes Against Children Training Conference.

4. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

STATUTORY AUTHORITY

5. As noted above, this investigation concerns alleged violations of the following:

- a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).
- b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

- a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This

feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-

BMS

trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

BMS

k. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions,

BMS

including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

s. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data

which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

7. On May 6, 2020, your affiant received a phone call from the Pasquotank County Sheriff's Office (PCSO) requesting assistance regarding a registered sex offender, Andrew HUFF (HUFF), who was found in possession of child pornography.

8. According to reports provided by PCSO, Probation and Parole Officer, Saul Turner advised PCSO that on Wednesday, May 06, 2020, at approximately 11:55 am, he went to a house call for Andrew HUFF, a registered sex offender, located at, 1206 Lakeside Dr., Elizabeth City, NC, 27909 (hereafter to be referred to as the SUBJECT RESIDENCE). Officer Turner advised that HUFF's ankle monitor was sending signals incorrectly and he wanted to check on the monitor. Officer Turner advised he approached HUFF at the SUBJECT RESIDENCE and observed a headset over his ears. Officer Turner advised HUFF he was not supposed to have a cellular phone and asked what the headset was attached to. HUFF stated the headset was hooked up to a CD player. Officer Turner advised that during this encounter a cellular phone rang. Officer Turner observed a white and silver iPhone (hereafter to be referred to as the SUBJECT DEVICE). Officer Turner asked HUFF who the SUBJECT DEVICE belonged to and HUFF admitted it belonged to him.

BMS

9. According to Officer Turner, HUFF is subject to warrantless searches as part of his supervised release. Officer Turner conducted a search of the SUBJECT DEVICE and observed a large amount of child pornography images and other sexually explicit images. Officer Turner advised that he also observed multiple conversations, from multiple unknown females on the SUBJECT DEVICE. All these findings were a violation of his probation requirements. Officer Turner confiscated the SUBJECT DEVICE and transported it to Pasquotank County Sheriff's Office.

10. PCSO Investigator Jason Wheelbarger spoke to Officer Turner at the Pasquotank County Sheriff's Office. Officer Turner stated he observed a collection of explicit photos on the SUBJECT DEVICE. Officer Turner described these photos as nude white females between the ages of five (5) and 18 with many females which appeared under the age of 16 years of age. Officer Turner stated he saw sexually explicit pictures of underage females in a bathtub, and in those images, he was able to see the female's naked breasts and vaginal areas. Officer Turner stated he observed over 600 images of what he believed was child pornography on the SUBJECT DEVICE. Officer Turner also observed several conversations HUFF was having with what appeared to be underage females. According to Officer Turner, many of these conversations included the exchanged of images, which consisted with nude pictures of what appeared to be underage females and HUFF's genitals. According to Officer Turner, HUFF has had a history of having children's

underwear and bras in his possession in his bedroom during previous searches of his residence.

11. On May 6, 2020, a violation was submitted to the Post Release and Parole Commission and an arrest warrant was issued for HUFF. HUFF was taken into custody and is currently being held at the Albemarle District Jail in Pasquotank County. During the jail booking process, HUFF wrote an apology letter which stated, in part, as follows:

"I, Andrew Huff was not intending to collect child pornography, I was searching them in the hopes of helping the police shut down all child pornography. I'm aware I went the wrong way about it, and I'm truly sorry. I've downloaded at least 500 or more to turn into the police, but was afraid of talking to the police, because of my record."

12. On May 6, 2020, PCSO Captain Brent McKecuen provided three separate CyberTips which had been reported to the National Center for Missing and Exploited Children (NCMEC). All three of the CyberTips were involving child pornography being traded via Facebook and Microsoft, Inc. The State Bureau of Investigation (SBI) sent Subpoenas to Internet Service Providers (ISP) for each of the CyberTips. According to SBI, all three CyberTips were linked to SUBJECT ADDRESS, where HUFF currently resides. No action had been taken by PCSO regarding these CyberTips yet.

13. Your affiant conducted a criminal history records check on HUFF and found that in 2010, HUFF was convicted in Indiana with Burglary and Sexual

Misconduct with a minor. HUFF was required to register as a sex offender for life. In 2017, HUFF was convicted in the Eastern District of North Carolina, of 3rd Degree Exploitation of a Minor (Felony), HUFF was sentenced to 36 months of supervised probation. In 2018, HUFF was convicted in the Eastern District of North Carolina of Soliciting a Child by Computer to Commit and Unlawful Sex Act (Felony) and 3rd Degree Exploitation of a Minor (Felony), HUFF was sentenced to one year and seven months in prison.

14. Your affiant obtained a copy of HUFF's Post Release Supervision Conditions, a seven-page document establishing conditions of his release, including:

"Do not use, possess, control, distribute, sell, exchange or collect child pornography and/or child erotica" and

"Submit at reasonable times to warrantless searches of any computer, telephone or electronic mechanism under my control."

Your affiant observed at the bottom of the page, HUFF signed acknowledgment of these conditions on February 6, 2019.

15. On May 11, 2020, your affiant observed a Facebook page which appears to belong to HUFF, according to his Facebook page he is in a relationship with a female who appears to be a senior in high school.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
AND THE INTERNET**

16. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic

communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any

BMS

computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in

BMS

the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on electronic devices. I know that electronic files, or remnants of such files, can be recovered months or even years after they have been downloaded onto a storage medium or electronic device, deleted, or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in

BMS

the file does not actually disappear; rather, the data remains on the storage medium or electronic device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten.

18. The warrant I am applying for would permit the examination of the item described in Attachment A consistent with Rule 41(e)(2)(B). The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the item, that might expose many parts of the item to human inspection in order to determine whether they contain evidence as described by the warrant.

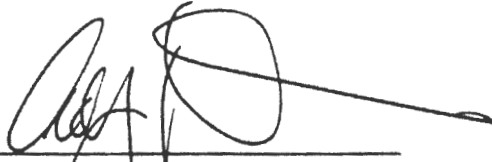
19. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT DEVICE described in Attachment A. I respectfully request that this Court issue a search warrant for the

BMS

SUBJECT DEVICE, authorizing the seizure and search of the items described in Attachment B.



Addy Penniman
Special Agent
Homeland Security Investigations

On this 13 day of May, 2020, Special Agent Addy Penniman appeared before me via reliable electronic means, was placed under oath, and attested to the contents of this Affidavit.



ROBERT B. JONES, JR.
United States Magistrate Judge

ATTACHMENT A

ITEMS TO BE SEARCHED

The device to be searched is a silver and white iPhone cell phone (IMEI # 356598080041281). The device is related to the investigation of Andrew HUFF and is in the custody of Homeland Security Investigations (HSI) at 721 Medical Center Drive, STE 300, Wilmington, North Carolina 28401.

BMS

ATTACHMENT B
ITEMS TO BE SEIZED

This warrant authorizes (i) the search of the property identified in Attachment A for only the following and (ii) authorizes the seizure of the items listed below only to the extent they constitute the following:

- (a) evidence of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) ("subject violations"); or
- (b) any item constituting contraband due to the subject violations, fruits of the subject violations, or other items possessed whose possession is illegal due to the subject violations; or
- (c) any property designed for use, intended for use, or used in committing any subject violations.

Subject to the foregoing, the items authorized to be seized include the following:

1. Child pornography, as defined in 18 U.S.C. § 2256(8).
2. Child erotica.
3. Records, information, and items relating to violations of the statutes described above in the form of:
 - a. Records and information referencing child pornography, as defined in 18 U.S.C. § 2256(8), and/or child erotica;
 - b. Records and information referencing or revealing the identity of the user.
 - c. Records and information referencing or revealing the owner or user of a Samsung cellular phone (model number SM-S727VL(GP)) smartphone;
 - d. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;
 - e. Records and information referencing or revealing a sexual interest in

BMS

children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

- f. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;
- g. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography; and
- h. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

4. Indicia of ownership and software programs on cellular phone:

- a. evidence of who used, owned, or controlled the cellular phone at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;
- b. evidence of how and when the cellular phone was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;
- c. evidence of the attachment to the cellular phone of other storage devices or similar containers for electronic evidence;
- d. evidence of the Internet Protocol addresses the cellular phone used to access the internet
- e. evidence of software that would allow others to control the cellular phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- f. evidence of the lack of such malicious software;
- g. evidence of programs (and associated data) that are designed to eliminate data from the cellular phone.